REMARKS

Claims 1-42 remain in this application. Applicants respectfully request reconsideration and review of the application in view of the following remarks.

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the patent application. The invention provides a form of data encryption/decryption in which the encrypted information can be decrypted only at a specified location. The location information is used to generate the key to encrypt and decrypt the information, referred to herein as a geolocking key. If someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information. The device performing the decryption determines its location using some sort of location sensor, such as a GPS receiver or other satellite or radio frequency positioning system.

More specifically, the patent application describes the use of a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that the digital information can be accessed in a decrypted form only at the specific geographic location. The location identity attribute may include a location value and a proximity value. The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions. The proximity value corresponds to a zone that encompasses the location. The location identity attribute may further include a temporal value such that the digital information can only be accessed at the specific geographic location and during a particular time period.

The digital information is encrypted and decrypted using a geolocking key based on the location identity attribute. The appliance that receives the encrypted digital information generates the geolocking key to decrypt the digital information based on its knowledge of the physical location of the appliance. Notably, the geolocking key is not

communicated to the receiving appliance—to the contrary, it is generated at the receiving end. If the appliance location is not within the proximate area of the location identity attribute, the appliance will be unable to generate the geolocking key to decrypt the digital information. More accurately, it will generate a key that will not be the right one to decrypt the digital information. By allowing decryption of the digital information only at the specific geographic location, the present invention enforces the location identity.

In accordance with certain embodiments of the invention, the proximity value of the location identity attribute further includes a shape parameter that defines a shape of a region that encompasses the specific geographic location in which the information is to be accessed. The shape parameter does not identify the location, so location cannot be discerned from the shape parameter alone. For example, the shape parameter may define the shape of the neighborhood in which the receiver is located, and all receivers in the same neighborhood may utilize the same shape parameter. The shape parameter is used along with the location data to generate the geolocking keys. This way, the shape parameter can be communicated to the receiving appliance along with the encrypted data. The receiving appliance would use the shape parameter along with its knowledge of its own geographic location (e.g., using a GPS receiver) to generate the geolocking key and thereby recover the encrypted information. Since the location data is not communicated, the geolocking key could not be generated by an unauthorized person that intercepts the communication and obtains the shape parameter.

The claims of the present application address both ends of the information communication process, i.e., encrypting (sending) end and decrypting (receiving) end. Independent Claims 1 and 22 each address the encryption of information at the sending end in respective method and apparatus claim forms. In contrast, independent Claims 14 and 34 each address the decryption of information at the receiving end in respective method and apparatus claim forms. Notably, the decryption claims further include

limitations directed to the use of the shape parameter.

The Examiner rejected Claims 1-42 under 35 U.S.C. § 102(b) as anticipated by Murphy. Applicants respectfully traverse this rejection.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated. Murphy further discloses: (a) updating or reconfiguring the licensed site location; (b) encasing the decryption module to prevent disassembly; (c) self-destruction of the decryption module upon attempted disassembly; and (d) notification of enforcement agency upon attempted unauthorized use.

There are very significant differences between Murphy and the present invention. First of all, Murphy does not disclose the encryption of data signals. To the contrary, the reference is directed solely to the decryption of encrypted signals. In fact, Murphy includes no discussion of the source of the encrypted signals other than that they are transmitted to the licensed sites by one or more satellites. See col. 7, lns. 23-26. Murphy therefore has no applicability whatsoever to independent Claims 1 or 22, which each address the encryption of information at the sending end of a communication system.

Second, Murphy does not use location information to generate a decryption key. Murphy does not generate a decryption key at all, since the decryption key is stored in the decryption module. Moreover, Murphy uses location information only to determine

whether to activate or deactivate the decryption key. The decryption key itself bears no relation to nor is it derived from the location information. In fact, the same decryption module (and decryption key) may be used for plural licensed sites with the only difference being the licensed site location coordinates that are programmed into the decryption module. Thus, Murphy discloses a system in which digital information is encrypted the same way for plural receivers. In contrast, the present invention provides a system in which digital information is specifically encrypted for each receiver using the location information unique to that receiver.

Third, Murphy does not encrypt or decrypt digital information using a geolocking key based on a location identity attribute. As discussed above, Murphy does not disclose how the signals are encrypted and the decryption key otherwise has no relation to the location information. The Murphy decryption key is entirely independent of location and therefore cannot reasonably be construed as a "geolocking key" as that term is used in the patent application. As a result, the encrypted digital information itself has no relationship with or association to the location information.
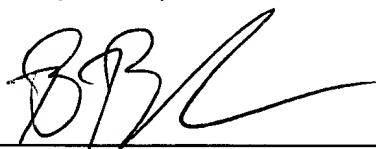
With respect to the Claims 1 and 22, Murphy fails to suggest or disclose, *inter alia,* the limitations of "generating a geolocking key based at least in part on said location identity attribute" and "encrypting said digital information using said geolocking key, wherein said encrypted digital information can be accessed only at said specific geographic location." Similarly, with respect to Claims 14 and 34, Murphy fails to suggest or disclose, *inter alia,* the limitations of "generating a geolocking key using at least said shape parameter and said location data" and "decrypting said digital information using said geolocking key." Accordingly, the rejection of Claims 1-42 over Murphy should be withdrawn.

In view of the foregoing, Applicants respectfully submit that Claims 1-42 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

While the Applicants believe that no fees are due in connection with the filing of this paper, the Commissioner is authorized to charge any shortage in the fees, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: October 12, 2004

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000